2020R00345/DEM/AMT/VSL

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. (SDW)
	:	
v.	:	Crim. No. 24-80
	:	
ARTUR SUNGATOV, and	:	18 U.S.C. § 371
IVAN KONDRATYEV,	:	18 U.S.C. § 1349
a/k/a "Ivan Gennadievich	:	18 U.S.C. § 1030(a)(5)(A)
Kondratiev,"	:	18 U.S.C. § 2
a/k/a "Ivan Kondratev,"	:	
a/k/a "Bassterlord"	:	

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges as follows:

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

Overview

1. From at least as early as in or around January 2020 through the present, defendants ARTUR SUNGATOV ("SUNGATOV"), IVAN KONDRATYEV, a/k/a "Ivan Gennadievich Kondratiev," a/k/a "Ivan Kondratev," a/k/a "Bassterlord" ("KONDRATYEV"), and others (collectively, the "Conspirators") were part of a conspiracy to deploy a ransomware variant known as "LockBit," a prolific form of malware and, at relevant times, the most deployed ransomware variant across the world. Since in or around January 2020 and continuing through the present, LockBit has been deployed against more than 2,000 victims, including victims in the District of New Jersey, and the Conspirators have received more than $120 million in ransom payments.

Relevant Individuals, Entities, and Terms

2. At times relevant to this Indictment:

a. SUNGATOV was a citizen of, and resided in, the Russian Federation.

b. KONDRATYEV was a citizen of the Russian Federation and resided in either Ukraine or the Russian Federation.

c. Mikhail Pavlovich Matveev ("Matveev"), also known as "Wazawaka," "m1x," "Boriselcin," and "Uhodiransomwar," a Conspirator who was previously charged for his participation in the LockBit conspiracy, was a citizen of, and resided in, the Russian Federation.

d. Mikhail Vasiliev ("Vasiliev"), a Conspirator who was previously charged for his participation in the LockBit conspiracy, was a citizen of both Canada and the Russian Federation and resided in Canada.

e. Application-1 was a file hosting service.

f. Application-2 was a social media platform where users could share and post text messages, images, and videos, as well as directly message other users.

g. Victim-1 was a law enforcement agency in Passaic County, New Jersey.

h. Victim-2 was a business in Dakota, Minnesota with operations and computers in New Jersey.

i. Victim-3 was a manufacturing company based in Zumbrota, Minnesota.

j. Victim-4 was a third-party logistics provider headquartered in Bloomington, Indiana.

k. Victim-5 was a manufacturing company based in Portland, Oregon.

l. Victim-6 was an insurance company based in San Juan, Puerto Rico.

m. Victim-7 was an intelligent automation and energy management solutions company with its headquarters in Waukesha, Wisconsin.

n. Victim-8 was a business in Essex County, New Jersey.

o. Victim-9 was a medical clinic based in Panama City, Florida.

p. Victim-10 was a hotel located in Sante Fe, New Mexico.

q. Victim-11 was a city in Puerto Rico.

r. Victim-12 was an engineering consulting services firm with an office in Morton, Illinois.

s. Victim-13 was a brokerage firm with its headquarters in New York, New York.

t. Victim-14 was a wholesale and distribution company with its headquarters in Singapore.

u. Victim-15 was a multinational semiconductor manufacturing company with its headquarters in Hsinchu, Taiwan.

v. Victim-16 was an international law firm with its headquarters in Beirut, Lebanon.

w. "Ransomware" was a type of malware that allowed a perpetrator to encrypt some or all of the data stored on a victim computer, transmit some or all of the victim's data to another computer under the perpetrator's control, or both. After a ransomware attack, a perpetrator would typically demand a ransom payment from the victim in exchange for decrypting the victim's data, deleting the perpetrator's copy of the victim's stolen data, or both.

The Conspiracy

3. From at least as early as in or around January 2020 through the present, in the District of New Jersey and elsewhere, the defendants

ARTUR SUNGATOV, and
IVAN KONDRATYEV,
a/k/a "Ivan Gennadievich Kondratiev,"
a/k/a "Ivan Kondratev,"
a/k/a "Bassterlord,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire and agree with each other and with Matveev, Vasiliev, and the other Conspirators to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a 1-year period from the Conspirators' course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a 1-year period, contrary to Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B)(i); and

b. to knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A).

Goal of the Conspiracy

4. The goal of the conspiracy was for SUNGATOV, KONDRATYEV, Matveev, Vasiliev, and the other Conspirators to enrich themselves by: (a) developing the LockBit ransomware variant, maintaining LockBit infrastructure (*e.g.*, computer servers and affiliate control panels, among other utilities) and hacking into and deploying LockBit against victim computer systems; (b) demanding and extracting ransom payments from victims following successful LockBit attacks; and (c) extorting noncompliant victims and intimidating future victims by, among other things, posting those victims' stolen data on the Internet through a website known as a "leak site" (the "LockBit Data Leak Site").

Manner and Means of the Conspiracy

5. It was part of the conspiracy that:

a. The LockBit conspiracy operates through the "ransomware-as-a-service" model, or "RaaS". The RaaS model involves two related groups of

ransomware perpetrators: developers and affiliates. The developers design the ransomware code itself, much as a software company would, and maintain the infrastructure, such as servers, on which LockBit operates. The developers then recruit and market their ransomware product to affiliates, who actually deploy the ransomware product designed by the developers.

b. The LockBit ransomware variant relies on a "control panel" for its operation. In the ransomware context, a "control panel" is a software dashboard made available to an affiliate by the developers to both provide that affiliate with tools necessary for the deployment of ransomware attacks and to allow developers to monitor their affiliates' activities. The LockBit control panel allowed affiliates, to, among other things, develop custom builds of the LockBit ransomware for particular victims, communicate with LockBit victims for ransom negotiation, and publish data stolen from LockBit victims to the LockBit Data Leak Site.

c. Much of the LockBit infrastructure, including the various LockBit control panels and the LockBit Data Leak Site, were hosted on the dark web. The "dark web" comprises Internet content that requires specialized software or configurations to access and is intended for anonymous and untraceable online communication.

d. Once a new affiliate joined the LockBit ransomware conspiracy, that affiliate was given their own control panel hosted at a unique domain name on the dark web.

e. A LockBit attack typically begins with affiliates gaining unauthorized access to vulnerable computer systems, through hacking, network

penetration techniques, and the use of stolen access credentials purchased from third parties. Affiliates then deploy LockBit within the victim computer systems, allowing affiliates to exfiltrate documents and data on the victim computer systems and to encrypt the data on the victim computer systems.

f. After LockBit has been deployed, affiliates leave behind a ransom note that provides the victim with instructions for how to contact the affiliate and a threat to publicly share the victim's stolen data and to leave the victim's data encrypted and thus inaccessible to the victim.

g. After ransom negotiations have begun, affiliates will demand a ransom payment in exchange for either decrypting the data on the victim's system and/or agreeing to not publicly post data exfiltrated from the victim system on the LockBit Data Leak Site. Affiliates typically demand payment in Bitcoin, a digital currency that allows Bitcoin holders to transfer their Bitcoin, stored at locations called "Bitcoin addresses," to other Bitcoin users at those users' Bitcoin addresses. As part of the Bitcoin framework, Bitcoin maintains a publicly available and reviewable ledger that records every Bitcoin transaction ever made, including sending and receiving Bitcoin addresses, date of transaction, and amount of Bitcoin transferred.

h. If the victim ultimately agrees to make a ransom payment, the affiliate typically sends the victim a Bitcoin address to send the demanded ransom. The affiliate and the developer will then split the payment between themselves. Typically, the developer receives 20% of the ransom payment and the affiliate receives 80% of the ransom payment.

Overt Acts

6. In furtherance of the conspiracy, and to effect its objects, Defendants and others committed the following overt acts, among others, in the District of New Jersey, and elsewhere:

a. On or about June 25, 2020, Matveev and the Conspirators deployed LockBit against Victim-1.

b. On or about September 14, 2020, Matveev and the Conspirators deployed LockBit against Victim-2.

c. In or around January 2021, SUNGATOV funded accounts on Application-1 that were used in connection with LockBit attacks on Victim-3 and Victim-4.

d. On or about January 12, 2021, SUNGATOV and the Conspirators deployed LockBit against Victim-3.

e. On or about January 29, 2021, SUNGATOV and the Conspirators deployed LockBit against Victim-4.

f. In or around August 2021, KONDRATYEV and the Conspirators deployed LockBit against Victim-5.

g. In or around August 2021, SUNGATOV and the Conspirators deployed LockBit against Victim-6.

h. On or about September 20, 2021, SUNGATOV and the Conspirators deployed LockBit against Victim-7.

i. On or about November 21, 2021, Vasiliev and the Conspirators deployed LockBit against Victim-8.

j. In or around June 2022, SUNGATOV and the Conspirators deployed LockBit against Victim-9.

k. On or about August 18, 2022, SUNGATOV and the Conspirators deployed LockBit against Victim-10.

l. In or around September 2022, KONDRATYEV and the Conspirators deployed LockBit against Victim-11.

m. On or about January 2, 2023, KONDRATYEV and the Conspirators deployed LockBit against Victim-12.

n. On or about April 10, 2023, KONDRATYEV, using an account at Application-2, publicly posted screenshots from inside the LockBit affiliate panel that depicted the attack on Victim-12.

o. In or around May 2023, KONDRATYEV and the Conspirators deployed LockBit against Victim-13.

p. On or about May 2, 2023, the LockBit Data Leak Site identified Victim-13 as a LockBit victim whose data would be published if Victim-13 did not pay the ransom demand. On or about May 11, 2023, KONDRATYEV sent direct messages to another user on Application-2 regarding the LockBit attack against Victim-13. Specifically, KONDRATYEV wrote: "I have a very large amount of data marked candy from their customers. They should pay soon. I'm just negotiating with the company at the moment."

q. In or around June 2023, KONDRATYEV and the Conspirators deployed LockBit against Victim-14.

r. In or around June 2023, KONDRATYEV and the Conspirators deployed LockBit against Victim-15.

s. In or around July 2023, KONDRATYEV and the Conspirators deployed LockBit against Victim-16.

All in violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud)

1. The allegations in paragraphs 1, 2, and 4 through 6 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. From at least as early as in or around January 2020 through the present, in the District of New Jersey and elsewhere, the defendants,

ARTUR SUNGATOV, and
IVAN KONDRATYEV,
a/k/a "Ivan Gennadievich Kondratiev,"
a/k/a "Ivan Kondratev,"
a/k/a "Bassterlord,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly and intentionally conspire with each other and with Matveev, Vasiliev, and the other Conspirators to devise, and intend to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

COUNTS 3 THROUGH 8
(Computer Fraud and Abuse)

1. The allegations in paragraphs 1, 2, and 4 through 6 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about each of the dates set forth below, the defendant,

ARTUR SUNGATOV,

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, described below for each Count, each transmission constituting a separate Count of this Indictment:

Count	Date(s)	Victim
Count 3	January 6, 2021 – January 29, 2021	Victim-3
Count 4	January 29, 2021 – February 11, 2021	Victim-4
Count 5	In or around August 2021	Victim-6
Count 6	September 20, 2021 – September 25, 2021	Victim-7
Count 7	In or around June 2022	Victim-9
Count 8	August 18, 2022 – September 20, 2022	Victim-10

In violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B)(i), and Section 2.

COUNTS 9 THROUGH 15
(Computer Fraud and Abuse)

1. The allegations in paragraphs 1, 2, and 4 through 6 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about each of the dates set forth below, the defendant,

IVAN KONDRATYEV,
a/k/a "Ivan Gennadievich Kondratiev,"
a/k/a "Ivan Kondratev,"
a/k/a "Bassterlord,"

who will first be brought to the District of New Jersey within the meaning of 18 U.S.C. § 3238, did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, described below for each Count, each transmission constituting a separate Count of this Indictment:

Count	Date(s)	Victim
Count 9	In or around August 2021	Victim-5
Count 10	In or around September 2022	Victim-11
Count 11	December 26, 2022 – January 31, 2023	Victim-12
Count 12	In or around May 2023	Victim-13
Count 13	In or around June 2023	Victim-14
Count 14	In or around June 2023 to in or around July 2023	Victim-15

Count 15	In or around July 2023	Victim-16

In violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B)(i), and Section 2.

FORFEITURE ALLEGATION AS TO COUNTS 1 AND 3 THROUGH 15

1. As a result of committing the offenses charged in Counts 1 and 3 through 15 of this Indictment, the defendants charged in each respective count, shall forfeit to the United States:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses charged in Counts 1 and 3 through 15 of this Indictment; and

b. pursuant to Title 18, United States Code, Section 1030(i), all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offenses charged in Counts 1, and 3 through 15 of this Indictment.

FORFEITURE ALLEGATION AS TO COUNT 2

2. As a result of committing the offense charged in Count 2 of this Indictment, the defendants,

ARTUR SUNGATOV, and
IVAN KONDRATYEV,
a/k/a "Ivan Gennadievich Kondratiev,"
a/k/a "Ivan Kondratev,"
a/k/a "Bassterlord,"

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the said offenses, and all property traceable thereto.

Substitute Assets Provision
(Applicable to All Forfeiture Allegations)

3. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third person;

(c) has been placed beyond the jurisdiction of the Court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be subdivided without difficulty,

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

A TRUE BILL

[redacted]

FOREPERSON

Philip R. Sellinger

PHILIP R. SELLINGER
United States Attorney

CASE NUMBER: 24-80(SDW)

United States District Court
District of New Jersey

UNITED STATES OF AMERICA
v.
ARTUR SUNGATOV, and
IVAN KONDRATYEV,
a/k/a "Ivan Gennadievich Kondratiev,"
a/k/a "Bassterlord"

INDICTMENT FOR
18 U.S.C. § 371
18 U.S.C. § 1349
18 U.S.C. § 1030(a)(5)(A)
18 U.S.C. § 2

A True Bill

[redacted]

Foreperson

PHILIP R. SELLINGER
UNITED STATES ATTORNEY
FOR THE DISTRICT OF NEW JERSEY

ANDREW M. TROMBLY
DAVID E. MALAGOLD
VINAY S. LIMBACHIA
ASSISTANT U.S. ATTORNEYS
NEWARK, NEW JERSEY

JORGE GONZALEZ
DEBRA IRELAND
TRIAL ATTORNEYS, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
WASHINGTON, DISTRICT OF COLUMBIA